UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,987	04/19/2004	Paul A. Gassoway	063170.7003	3477

5073 7590 08/19/2009

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
ZEE, EDWARD	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
08/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/826,987	GASSOWAY, PAUL A.	
	Examiner	Art Unit	
	EDWARD ZEE	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26 and 30-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26 and 30-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendments filed on 06/01/09. Claims 1, 4, 9, 16 and 34 have been amended; Claims 27-29 have been cancelled; Claim 35 has been added; Claims 1-26 and 30-35 are pending and have been considered below.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/01/09 has been entered.

Claim Objections

3. **Claim 16** is objected to because of the following informalities: the Examiner notes that the instant claim currently recites, "A tangible computer storage medium...comprising", and may potentially encompass non-statutory subject matter, which does not appear to be the Applicant's intent. The Applicant is kindly requested to clarify the claim by amending the claim to recite, "A tangible computer storage medium...the computer executable code comprising" or the like. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claims 9, 10, 14, 17-23, 31 and 32** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. **Claim 9** recites the limitation "the web server" throughout the claim. There is insufficient antecedent basis for this limitation in the claim. The Examiner respectfully notes that there appears to be at least two separate instances of "a web server" recited in the instant claim(lines 6 and 8 respectively), and thus may be unclear which web server such a limitation is in reference to.

7. **Claims 10 and 14** recite the limitation "the proxy machine" in line 1. There is insufficient antecedent basis for this limitation in the claim.

8. **Claims 17-23** recite the limitation "the computer recording medium" in line 1. There is insufficient antecedent basis for this limitation in the claim.

9. **Claims 31 and 32** recites the limitation "the viral signature patterns" throughout the claims. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1-5, 9-11, 15-20, 24-26, 30-32, 34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kindberg et al. (2003/0061515) in view of Haugh (7,231,666) and Thiele et al. (2005/0050353).

Claim 1: Kindberg et al. discloses a method for maintaining computer security comprising:

a. providing a signature file*(ie. a database containing capabilities, etc.)* containing information about known system vulnerabilities*(ie. acceptable arguments for a CGI script)* [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. at a reverse proxy server residing between at least one client computer and a web server [figure 2]:

i. receiving an incoming message from the at least one client computer, wherein the incoming message, if malicious and upon receipt by the web server, automatically causes the web server to perform an action which exploits a vulnerability of the web server*(ie. step 600)* [figure 6];

ii. comparing the received incoming message with the signature file to determine whether the incoming message is malicious*(ie. step 610)* [figure 6];

iii. and if it is determined to be malicious, blocking the incoming message from reaching the web server*(ie. request is rejected)* [page 4, paragraph 0054].

Additionally, Kindberg et al. further discloses that the signature file may also include arguments to explicitly exclude which fairly suggests including "signatures" of malicious messages to block or the like [page 5, paragraph 0059]; but does not explicitly disclose that the signature file contains information comprising a predefined length of a Universal Resource Location for a message header; nor comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file and if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server.

Nonetheless, Haugh discloses a similar invention and further discloses preventing buffer overflow security exploits by utilizing a signature file containing information comprising a predefined length of an argument*(ie. hard limit)*; comparing a length of an argument with the predefined length in the signature file and if the length exceeds the predefined length*(ie. if the length of the command line argument being processed exceeds a hard limit)*, blocking the argument [column 5, lines 50-55 & figure 5].

Furthermore, Thiele et al. discloses that common computer attacks include buffer overflow attacks, malformed URL attacks and forming "signatures" to characterize such attacks [page 1, paragraphs 0002 & 0008].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify invention disclosed by Kindberg et al. with the additional features disclosed by Haugh, in order to facilitate the identification and prevention of buffer overflow attacks, as suggested by Thiele et al. [page 1, paragraph 0005].

Claim 9: Kindberg et al. discloses a system for maintaining computer security comprising:

a. a signature file containing information about known system vulnerabilities, the information not including viral signature patterns [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. a web server [figure 2];

c. reverse proxy server residing on a processor controlled device between at least one client computer and a web server, the reverse proxy server operable to [figure 6]:

i. receiving an incoming message from the at least one client computer, wherein the incoming message, if malicious and upon receipt by the web server, automatically

causes the web server to perform an action which exploits a vulnerability of the web server [figure 6];

ii. comparing the received incoming message with the signature file to determine whether the incoming message is malicious [figure 6];

iii. and if it is determined to be malicious, blocking the incoming message from reaching the web server [page 4, paragraph 0054].

Additionally, Kindberg et al. further discloses that the signature file may also include arguments to explicitly exclude which fairly suggests including "signatures" of malicious messages to block or the like [page 5, paragraph 0059]; but does not explicitly disclose that the signature file contains information comprising a predefined length of a Universal Resource Location for a message header; nor comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file and if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server.

Nonetheless, Haugh discloses a similar invention and further discloses preventing buffer overflow security exploits by utilizing a signature file containing information comprising a predefined length of an argument*(ie. hard limit)*; comparing a length of an argument with the predefined length in the signature file and if the length exceeds the predefined length*(ie. if the length of the command line argument being processed exceeds a hard limit)*, blocking the argument [column 5, lines 50-55 & figure 5].

Furthermore, Thiele et al. discloses that common computer attacks include buffer overflow attacks, malformed URL attacks and forming "signatures" to characterize such attacks [page 1, paragraphs 0002 & 0008].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify invention disclosed by Kindberg et al. with the additional features disclosed by Haugh, in order to facilitate the identification and prevention of buffer overflow attacks, as suggested by Thiele et al. [page 1, paragraph 0005].

Claim 16: Kindberg et al. discloses a computer storage medium containing code for maintaining computer security comprising:

a. providing a signature file containing information about known system vulnerabilities, the information not including viral signature patterns [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. at a HTTP reverse proxy server residing between at least one client computer and a web server [figure 2]:

i. receiving an incoming message from the at least one client computer, wherein the incoming message, if malicious and upon receipt by the web server, automatically causes the web server to perform an action which exploits a vulnerability of the web server [figure 6];

ii. comparing the received incoming message with the signature file to determine whether the incoming message is malicious [figure 6];

iii. and if it is determined to be malicious, blocking the incoming message from reaching the web server [page 4, paragraph 0054].

Additionally, Kindberg et al. further discloses that the signature file may also include arguments to explicitly exclude which fairly suggests including "signatures" of malicious messages to block or the like [page 5, paragraph 0059]; but does not explicitly disclose that the signature file contains information comprising a predefined length of a Universal Resource Location for a message header; nor comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file and if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server.

Nonetheless, Haugh discloses a similar invention and further discloses preventing buffer overflow security exploits by utilizing a signature file containing information comprising a predefined length of an argument*(ie. hard limit)*; comparing a length of an argument with the predefined length in the signature file and if the length exceeds the predefined length*(ie. if the length of the command line argument being processed exceeds a hard limit)*, blocking the argument [column 5, lines 50-55 & figure 5].

Furthermore, Thiele et al. discloses that common computer attacks include buffer overflow attacks, malformed URL attacks and forming "signatures" to characterize such attacks [page 1, paragraphs 0002 & 0008].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify invention disclosed by Kindberg et al. with the additional features disclosed by Haugh, in order to facilitate the identification and prevention of buffer overflow attacks, as suggested by Thiele et al. [page 1, paragraph 0005].

Claim 34: Kindberg et al. discloses a method for maintaining computer security comprising:

a. providing a signature file containing information about known system vulnerabilities the information comprising a predefined length of a Universal Resource Locator ("URL") in a message header [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. receiving an incoming message from at least one client computer [figure 6];

c. comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file to determine whether the incoming message is malicious*(ie. URL having a character string conforming to the length established)* [page 4, paragraph 0052];

d. and if the incoming message is determined to be malicious, blocking the incoming message from reaching a web server [page 4, paragraph 0054].

Additionally, Kindberg et al. further discloses that the signature file may also include arguments to explicitly exclude which fairly suggests including "signatures" of malicious messages to block or the like [page 5, paragraph 0059]; but does not explicitly disclose that the signature file contains information comprising a predefined length of a Universal Resource Location for a message header; nor comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file and if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server.

Nonetheless, Haugh discloses a similar invention and further discloses preventing buffer overflow security exploits by utilizing a signature file containing information comprising a predefined length of an argument*(ie. hard limit)*; comparing a length of an argument with the predefined length in the signature file and if the length exceeds the predefined length*(ie. if the*

length of the command line argument being processed exceeds a hard limit), blocking the argument [column 5, lines 50-55 & figure 5].

Furthermore, Thiele et al. discloses that common computer attacks include buffer overflow attacks, malformed URL attacks and forming "signatures" to characterize such attacks [page 1, paragraphs 0002 & 0008].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify invention disclosed by Kindberg et al. with the additional features disclosed by Haugh, in order to facilitate the identification and prevention of buffer overflow attacks, as suggested by Thiele et al. [page 1, paragraph 0005].

Claims 2-4, 10 and 17-19: Kindberg et al., Haugh and Thiele et al. disclose an invention as in claims 1, 9 and 16 above and Kindberg et al. further discloses that the comparing further comprises:

a. parsing the incoming message [page 4, paragraph 0055];

b. converting the incoming message into an internal format*(ie. specific CGI arguments etc.)* [page 5, paragraph 0060];

c. comparing the converted incoming message with the signature file and determining whether the converted incoming message is malicious based on the comparison*(ie. list of acceptable arguments etc)* [page 5, paragraph 0059];

d. reassembling the converted incoming message back into its original format prior to forwarding it to the web server if it is determined that the code is not malicious and forwarding the reassembled message to the web server*(ie. arugment passed through unchanged, etc.)* [page 5, paragraph 0061].

Claims 5, 11 and 20: Kindberg et al., Haugh and Thiele et al. disclose an invention as in claims 1, 9 and 16 above and Kindberg et al. further discloses that the signature file contains information about known system vulnerabilities*(ie. acceptable arguments for a CGI script)* [page 4, paragraph 0054 & page 5, paragraphs 0058-0059].

Claim 15: Kindberg et al., Haugh and Thiele et al. disclose a system as in claim 10 above and Kindberg et al. further discloses that the signature file is linked to the HTTP message analyzer module*(ie. list of acceptable arguments)* [page 5, paragraph 0058].

Claims 24-26: Kindberg et al., Haugh and Thiele et al. disclose a method, system and computer storage medium as in claims 1, 9 and 16 above, and Kindberg et al. further discloses that the incoming message comprises an HTTP messages [abstract].

Claims 30-32: Kindberg et al., Haugh and Thiele et al. disclose the invention of claims 1, 9 and 16, and Kindberg et al. further discloses that the information comprises a list of known system vulnerabilities; and comparing the received incoming message with the signature file to determine whether the incoming message is malicious comprises determining whether the incoming message is malicious by determining whether one or more characteristics of the incoming message satisfy one of the vulnerabilities on the list of known system vulnerabilities*(ie. character string length is not a bogus argument, etc.)* [page 5, paragraph 0058-0059].

Claim 35: Kindberg et al., Haugh and Thiele et al. disclose a method as in claim 34 above and Haugh further discloses:

a. the predetermined length indicates a maximum amount of data that may be stored in a buffer of the web server before the buffer overflows*(ie. components used in preventing exploits*

based on buffer overflow...places limitations on the size of individual input parameters to prevent arguments from exceeding a selected size) [column 3, lines 63-67 | column 4, lines 1-5];

b. the length of the incoming URL indicates an amount of data that the incoming message will attempt to store on the buffer if the incoming message is received by the web server*(ie. if length does exceed hard limit)* [column 5, lines 50-55]; and

c. the step of determining that the incoming message is malicious comprises determining that the incoming message is capable of causing the buffer to overflow*(ie. a security action is performed in response to detecting data for the data buffer having a size greater than a designated size)* [column 1, lines 63-67].

12. Claims 6-8, 12-14 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kindberg et al. (2003/0061515) in view of Haugh (7,231,666) and Thiele et al. (2005/0050353) and further in view of Cambridge (7,080,000).

Claims 6, 12 and 21: Kindberg et al., Haugh and Thiele et al. disclose a method, system and computer storage medium as in claims 1, 9 and 16 above, but does not explicitly disclose that the signature file is made available through a web server. However, Cambridge discloses a similar method, system and computer storage medium and further discloses that the signature file*(antivirus database)* is made available through a web server*(antivirus server)* [abstract]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to make the signature files available through a web server. One would have been motivated to do so in order to make signature file updates easily accessible.

Claims 7, 13 and 22: Kindberg et al., Haugh and Thiele et al. disclose a method, system and computer storage medium as in claims 1, 9 and 16 above, but does not explicitly disclose

continuously updating the signature file. However, Cambridge discloses a similar method, system and computer storage medium and further discloses continuously updating the signature file*(antivirus data file)* [column 2, lines 63-67]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to continuously update the signature file. One would have been motivated to do so in order to be able to detect the latest viruses, which are constantly being created.

Claims 8, 14 and 23: Kindberg et al., Haugh and Thiele et al. disclose a method, system and computer storage medium as in claims 1, 9 and 16 above, but does not explicitly disclose periodically downloading the signature file in order to make its copy current. However, Cambridge discloses a similar method, system and computer storage medium and further discloses periodically downloading the signature files*(receiving a new antivirus file at one of the user computers)* in order to make its copy current [abstract]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to periodically download the signature files. One would have been motivated to do so in order to be able to detect the latest viruses, which are constantly being created.

13. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kindberg et al. (2003/0061515) in view of Haugh (7,231,666) and Thiele et al. (2005/0050353) and further in view of El-Rafie (6,968,394).

Claim 33: Kindberg et al., Haugh and Thiele et al. disclose the method of claim 1, and Kindberg et al. further discloses logging user requests and in particular logging the user identity [page 4, paragraph 0056], but does not explicitly disclose that if the incoming message is determined to

be malicious, identifying the first computer; and automatically blocking future messages received from the first client computer.

However, El-Rafie discloses a similar method and further discloses monitoring requests and identifying/blocking malicious users from future requests*(ie. determining rogue user terminals and blocking data flow to the offending IP address, etc.)* [column 26, lines 10-61].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the method disclosed by Kindberg et al. with the features disclosed by El-Rafie in order to automatically provide a more selective access to resources within a network, as suggested by Kindberg et al. [page 1, paragraph 0012].

Response to Arguments

14. Applicant's arguments with respect to the pending claims have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
August 10, 2009
/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435